INFO

Les ennemis de Dieu ont utilisé toutes les méthodes pour affronter les moudjahidines. Le journaliste Shane Harris a publié dans son célèbre livre @WAR au cours de la croisade contre l'Irak l'Agence de sécurité nationale des États-Unis a publié un programme d'amalgame dans un forum des jihadiste pour pouvoir pénétrer les visiteurs moudjahidin sur le site afin de rechercher des informations et de les localiser.

Vérification de l'empreinte digitale numérique pour les applications Android

الحمدللَّه معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره ومستدرج الكافرين بمكره الذي قدر الايام دولا بعدله وجعل العافية للمتقين بفضله والصلاة والسلام على من أعلى اللَّه منار الاسلام بسيفه وعلي اله وصحبه ومن تبعهم باحسان الي يوم الدين اما بعد

Index de l'article

Les étapes pour extraire l'application en tant que fichier APK.

La première application est hashbot

La deuxième application est hashdroid

La troisième application est hashr

Vérification de l'empreinte digitale numérique pour les applications Android

Introduction:

Les ennemis de Dieu ont utilisé toutes les méthodes pour affronter les moudjahidines. Le journaliste Shane Harris a publié dans son célèbre livre @WAR au cours de la croisade contre l'Irak l'Agence de sécurité nationale des États-Unis a publié un programme d'amalgame dans un forum des jihadiste pour pouvoir pénétrer les visiteurs moudjahidin sur le site afin de rechercher des informations et de les localiser. Internet est un espace médiatique pour les moudjahidines, à travers lequel ils propagent la réalité de leurs actions loin de la diffamation et du mensonge que nous voyons sur les chaînes satellites, les journaux et les magazinesCe que nous voyons par le biais de chaînes satellites, de journaux, de magazines et de sites Web a donc compris l'importance d'Internet et développé et programmé des applications pour diffuser des informations sur les batailles et publications, mais exploité les ennemis de Dieu dans le déploiement d'applications bombardées entre les partisans et leurs partisans afin de leur permettre de se tromper et de récupérer leurs données. donc vous devez faire, vous devez vérifier l'empreinte numérique de l'application avant de l'installer sur votre appareil.

Empreinte numérique:

Il s'agit d'une marque de sécurité électronique qui repose sur la cryptographie pour créer une signature numérique pour les fichiers. Cette signature peut être ajoutée aux fichiers ou aux applications, ce qui vous permet de vérifier l'éditeur du fichier. Elle permet également de vérifier que le fichier n'a pas été modifié depuis sa signature ou sa modification Si le fichier ou l'application a été modifié ou non via l'empreinte numérique)

Comment vérifier l'empreinte numérique sur le système Android:

Vous pouvez vérifier l'empreinte numérique des fichiers à l'aide de l'une des applications suivantes:

| Hashr

| HashBot

| Hashdroid)

Étapes d'extraction de l'application APK:

▪ Tout d'abord, extrayez l'application officielle installée sur le périphérique (téléchargée à partir de Google Play ou d'une source fiable) sous forme de fichier via l'application ML Manager qui extrait l'application installée sur votre périphérique sous la forme d'un fichier.

▪ Les applications installées sur votre appareil apparaîtront sur l'interface de ML Manager Cliquez sur SHARE APK pour partager l'application ou sur EXTRACT pour extraire et enregistrer le format APK sur votre appareil.

▪ Les applications seront conservées après avoir été extraites dans un dossier nommé ML Manager.

• Pour comparer l'empreinte numérique entre les applications source officielles et la source anonyme, nous avons téléchargé la même version de l'application en tant que fichier APK depuis l'un des canaux (source anonyme) pour vérifier sa signature et voir si elle a été modifiée en premier.

• Note:

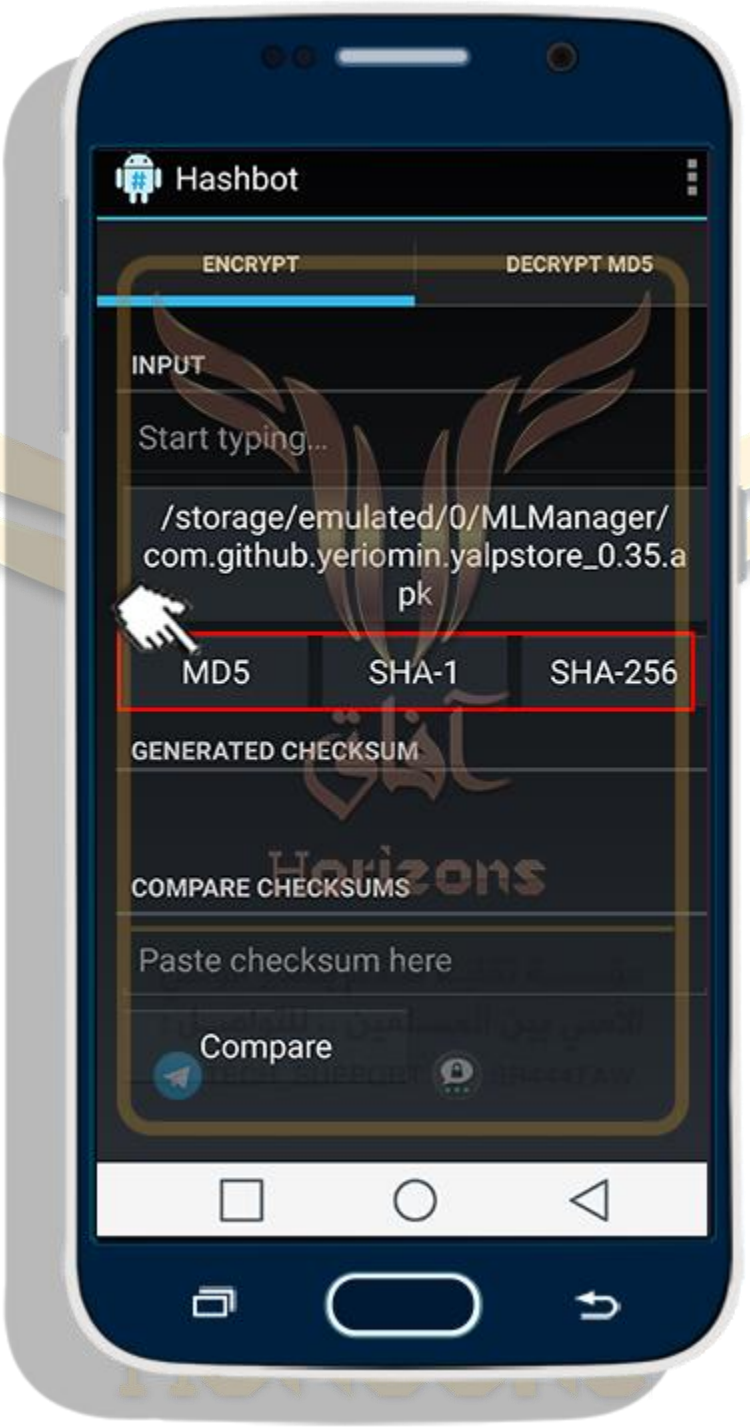
Évitez d'installer des applications ou d'ouvrir des fichiers avec une balise différente de la source officielle de l'application. Vous pourriez être victime d'un piratage pour cette raison et télécharger à partir de sources ou de magasins fiables

Première application:

Hashbot

- Pour télécharger l'application Hashbot à partir du Google Play Store, cliquez ici.
- Appuyez sur Or choose file pour le sélectionner.
- Sélectionnez le fichier que vous souhaitez vérifier.

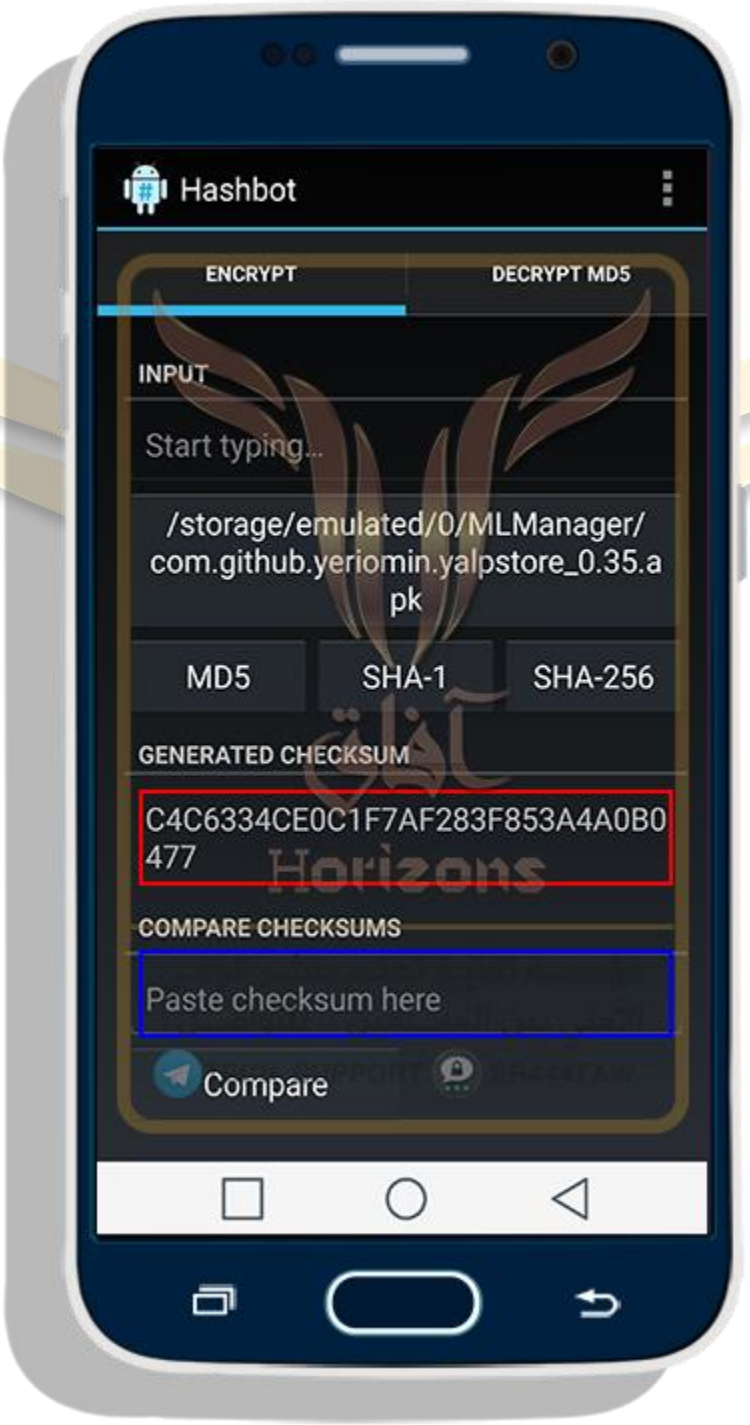
▪ Choisissez l'algorithme dans lequel le fichier est signé et vous avez une valeur. Par exemple, je choisirai l'algorithme MD5.



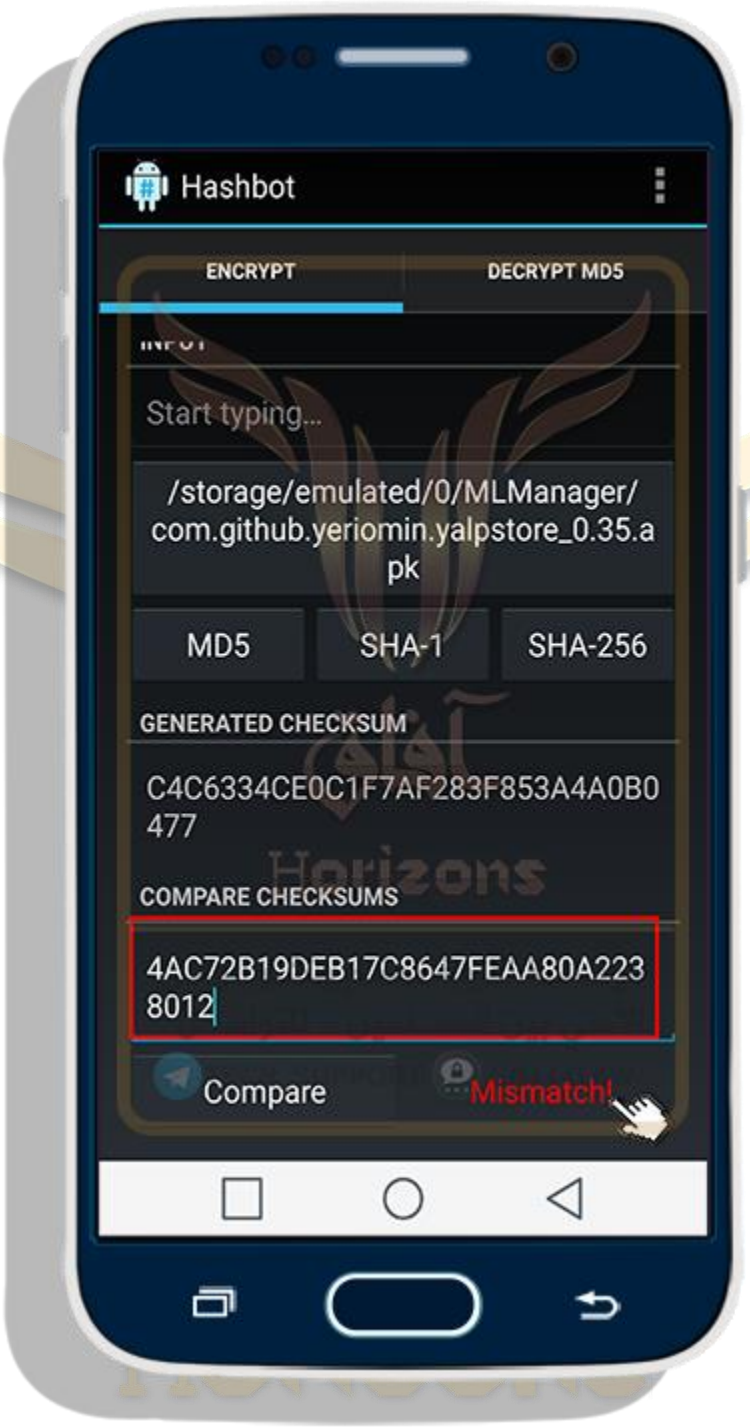
▪ Vous verrez l'empreinte numérique du fichier avec l'algorithme MD5, comme indiqué dans l'encadré rouge.

▪ Dans la zone bleue, copiez l'empreinte numérique du fichier que vous souhaitez comparer avec la version officielle.

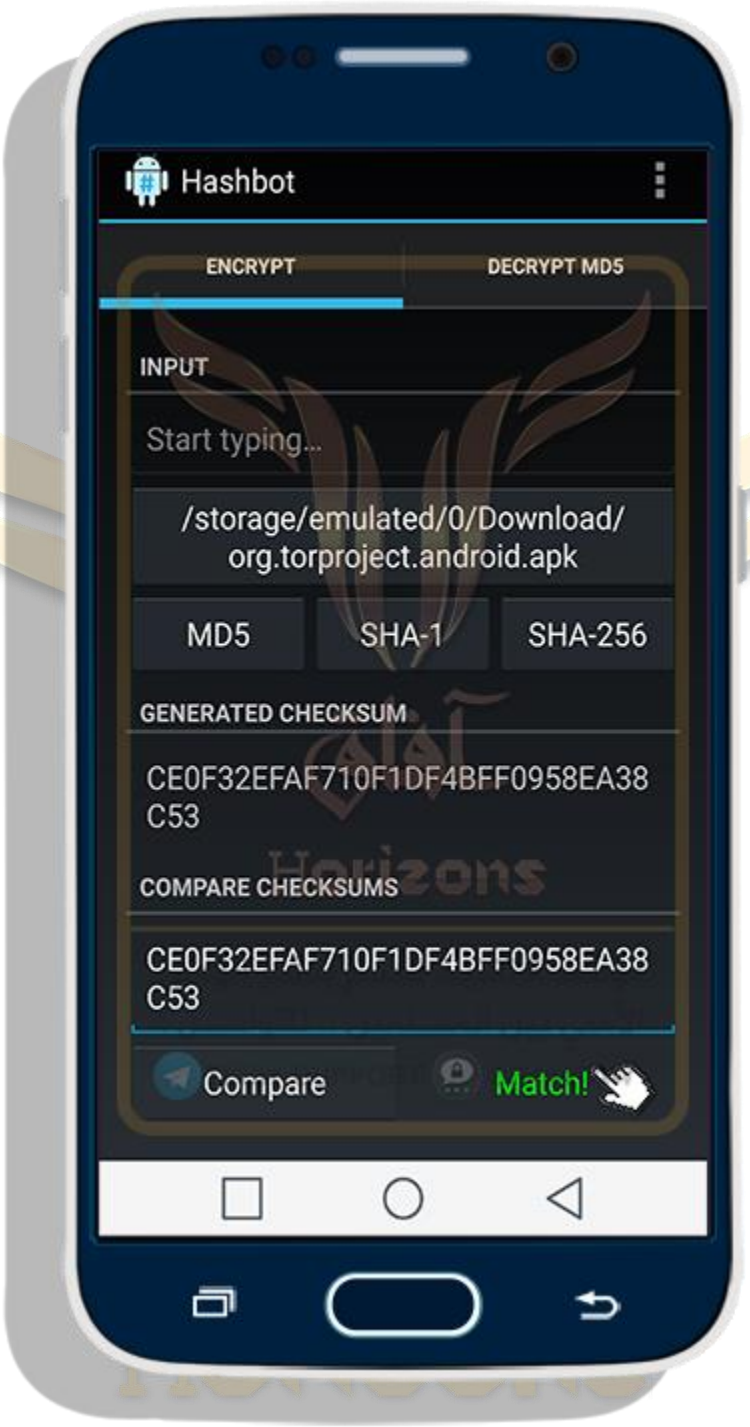
▪ Nous copierons l'empreinte numérique du fichier que nous avons téléchargé à partir de l'un des canaux (source anonyme).



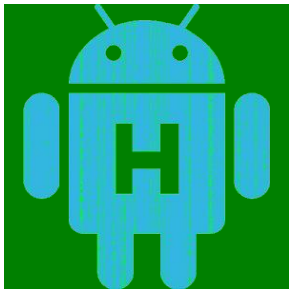
▪ Si le résultat indique Mismatch! Cela signifie que l'empreinte digitale n'est pas identique et que l'application a été modifiée.



▪ ▪ Si le résultat montre Match telle que présentée dans l'image suivante, les deux images sont identiques et l'application n'est pas modifiée.



Deuxième application:

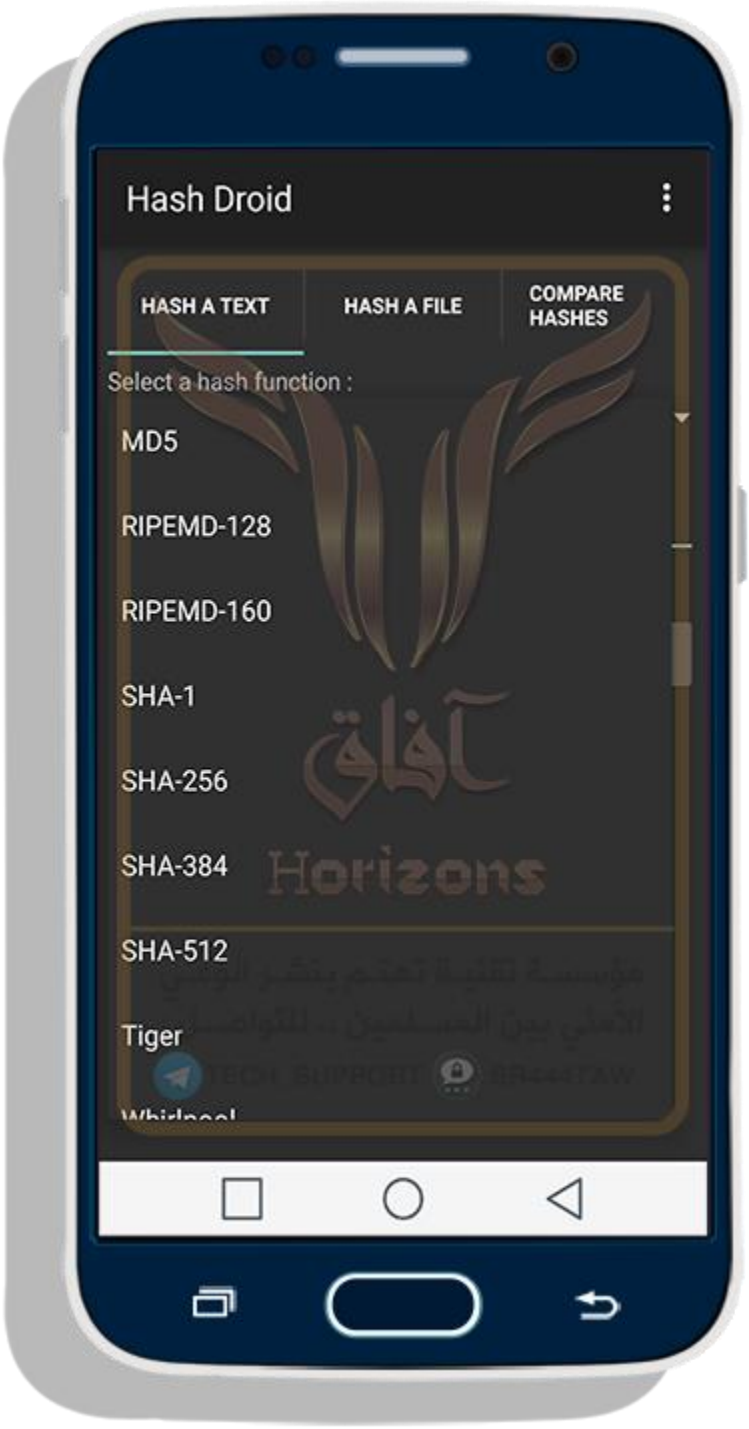


Hashdroid

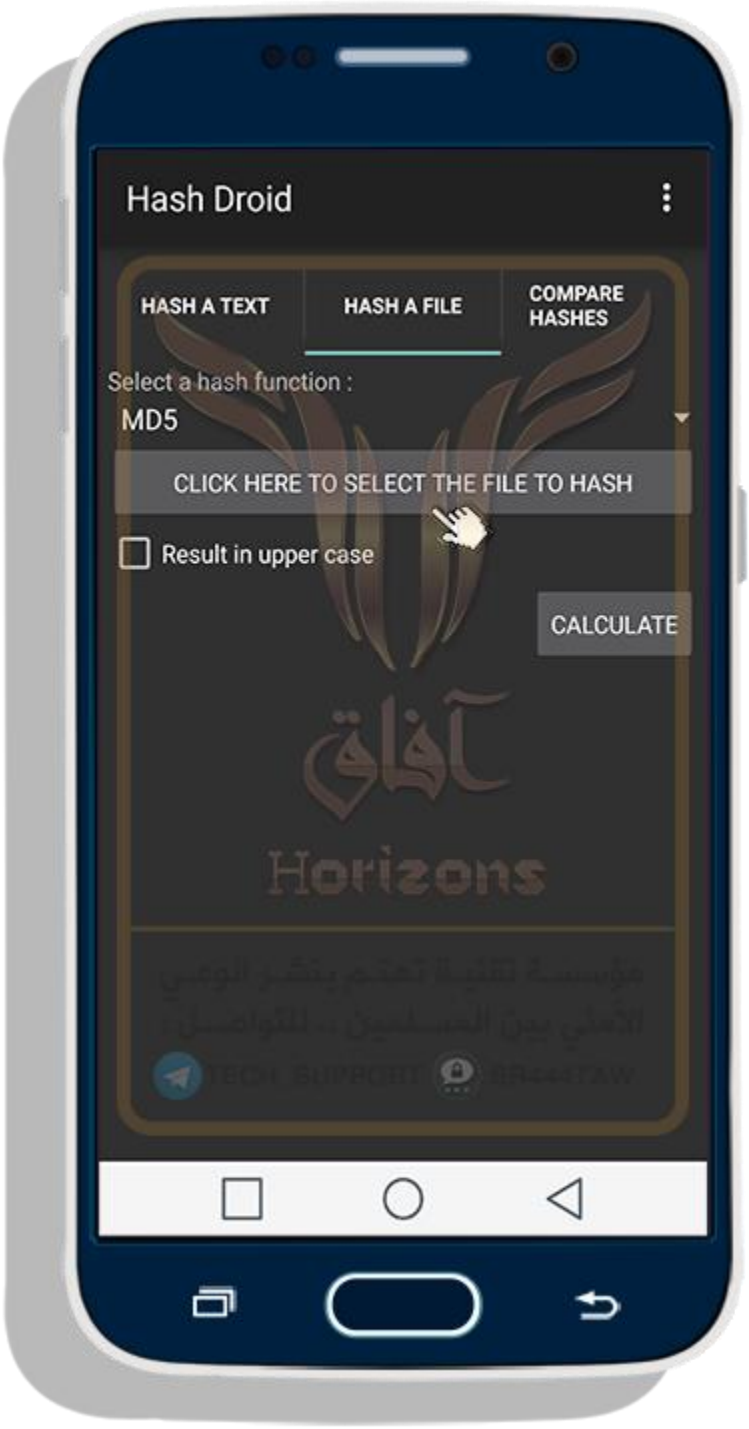
▪ Nous avons d'abord téléchargé un fichier APK depuis un canal (source anonyme).

▪ Nous avons téléchargé la même application et la même version mais à partir d'une source fiable.

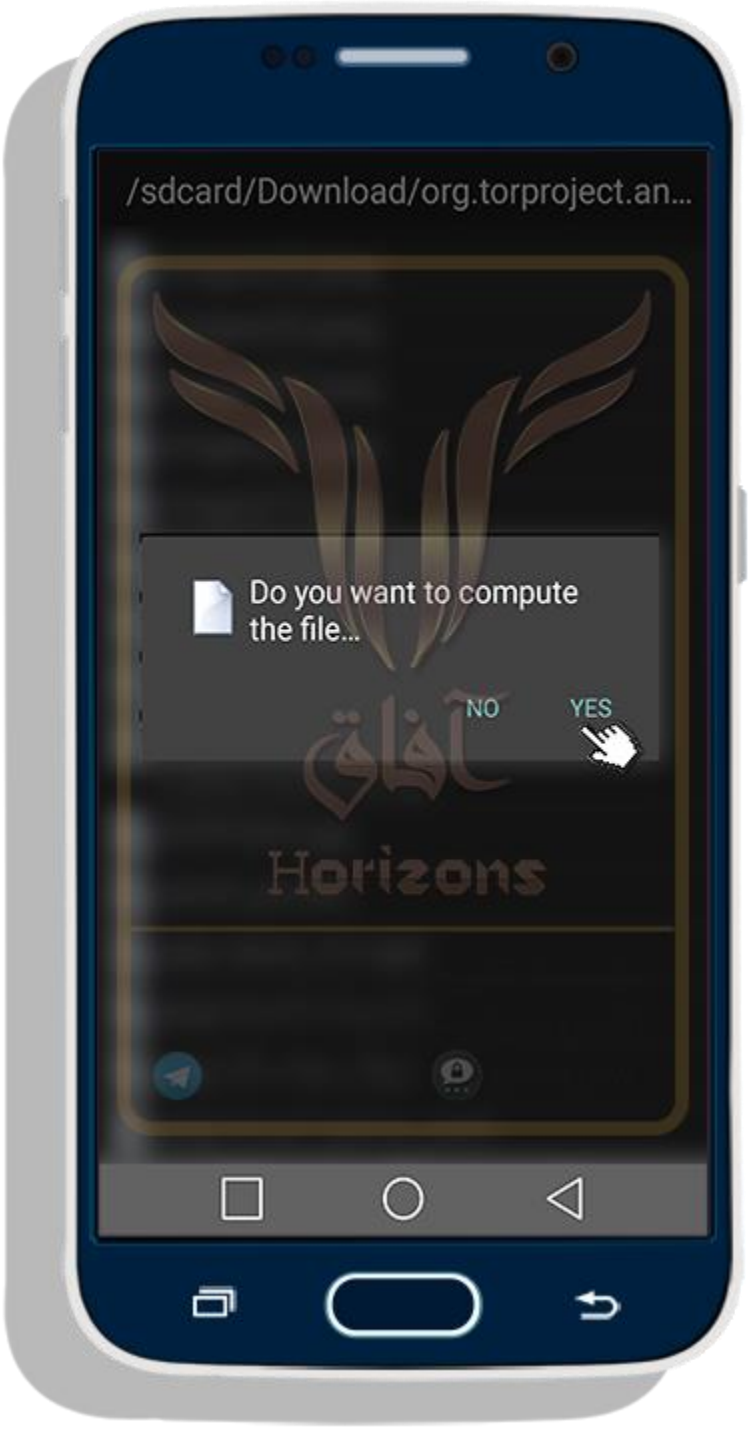
▪ Cliquez sur l'emplacement indiqué et sélectionnez l'algorithme dans lequel le fichier a été signé et qui a une valeur. Par exemple, je choisirai l'algorithme MD5.



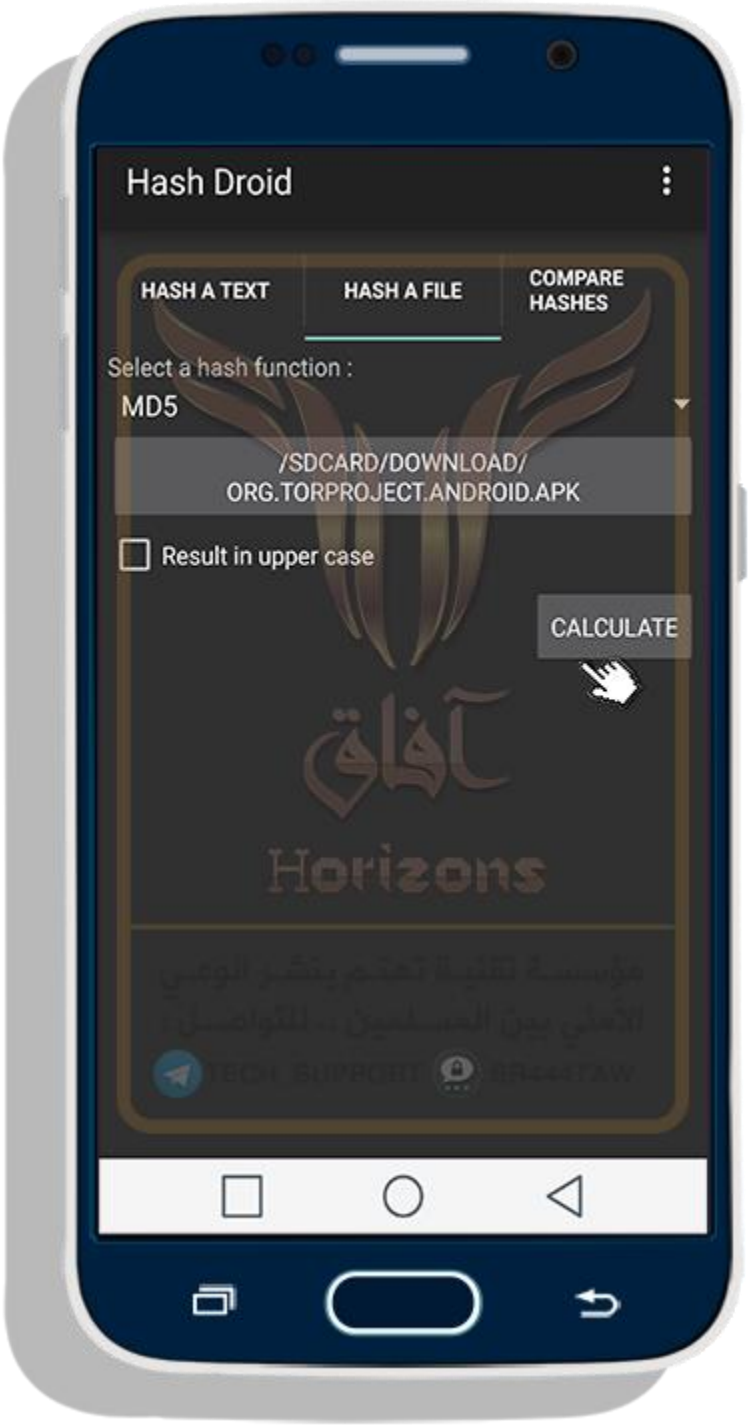
▪ Pour sélectionner le fichier, appuyez sur **CIICK HERE TO SELECT THE FILE TO HASH**



- Appuyez sur YES



- Appuyez sur **CALCULATE**

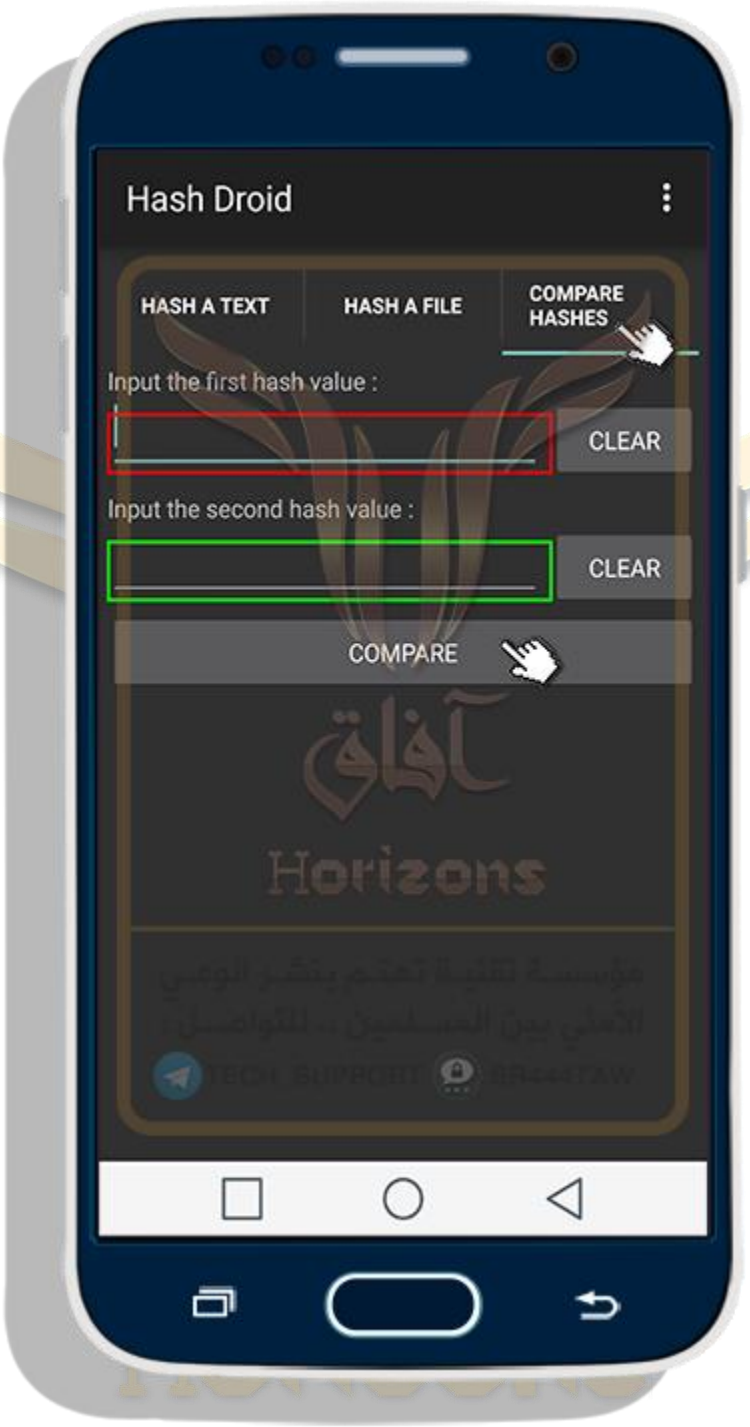


• L'empreinte numérique apparaîtra devant MD5 checksum

▪ Appuyez sur COPY CHECKSUM TO CLIPBOARD pour copier l'empreinte numérique.

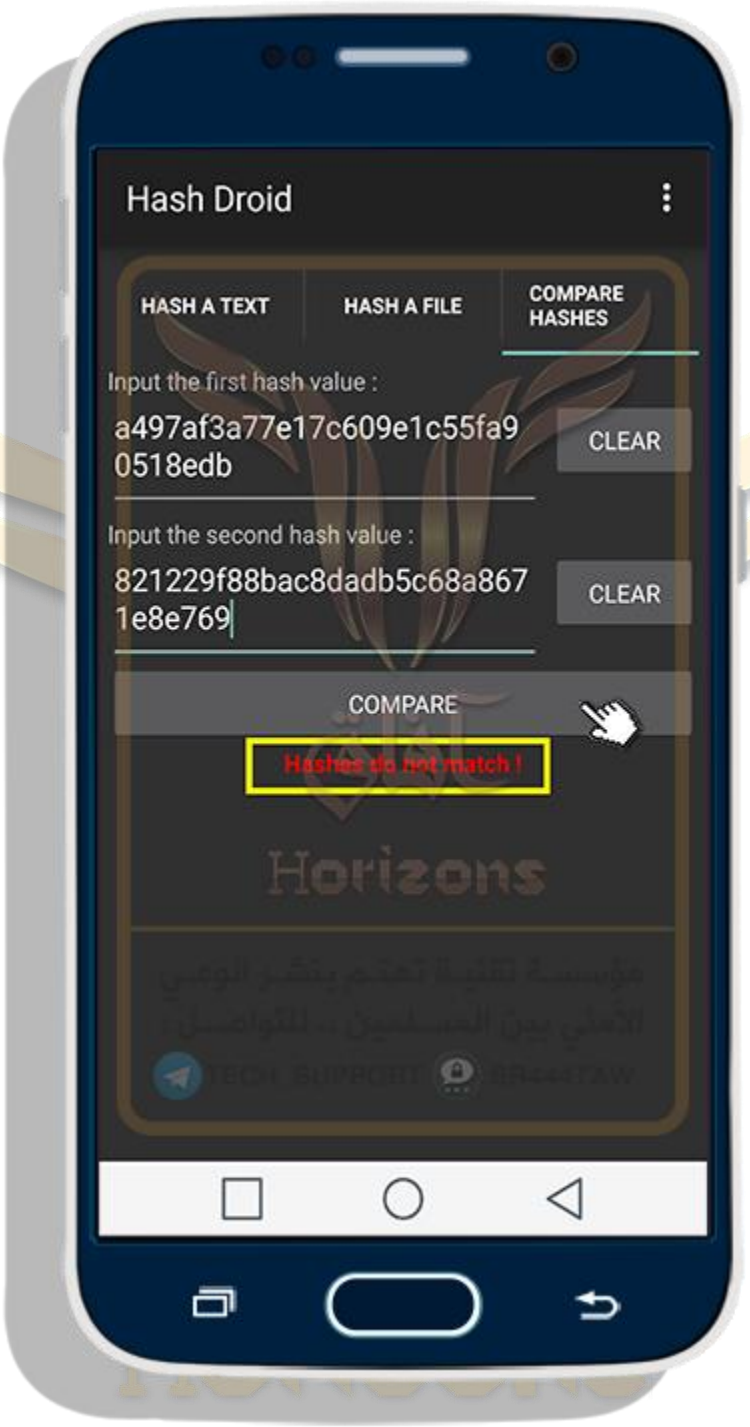
▪ Appuyez sur COMPARE HASHES et copiez l'empreinte dans la case rouge.

▪ Copiez l'empreinte numérique du fichier que vous souhaitez comparer.



▪ Appuyez sur COMPARE

▪ Si le résultat apparaît Hashes do not match donc l'empreinte digitale n'est pas compatible



▪ S'il apparaît **Hashes match** Cela signifie que l'empreinte est compatible

Troisième application:

Hashr

▪ Pour télécharger l'application Hashr à partir du Google Play Store, cliquez ici.

▪ Pour télécharger l'application Hashr à partir du magasin Druid, cliquez ici.

▪ Cliquez sur l'emplacement indiqué dans l'image suivante

• Les paramètres **From Text** pour comparer l'empreinte numérique du texte sans ajouter de fichiers

• Les paramètres **From File** pour afficher et comparer l'empreinte numérique d'un fichier.

• Choisissez le type d'empreinte à vérifier pour le fichier, choisissez SHA-256.

▪ Cliquez sur l'emplacement indiqué dans l'image ci-dessous pour sélectionner un fichier et appuyez sur GENERATE pour afficher l'empreinte numérique du fichier.

▪ Copiez l'empreinte numérique pour la comparer à l'empreinte du fichier à l'emplacement indiqué.
▪ Appuyez ensuite sur SHA-256 HASHES Compare

▪ Si le résultat de la comparaison de l'image de correspondance Match apparaît en vert, comme indiqué dans l'image, donc l'empreinte numérique du fichier est identique à l'empreinte de texte que vous avez copiée, le fichier n'est pas modifié par les autres parties.

▪ Si le résultat de la comparaison de l'image de correspondance Match apparaît en vert, comme indiqué dans l'image, donc l'empreinte numérique du fichier est identique à l'empreinte de texte que vous avez copiée, le fichier n'est pas modifié par les autres parties.

******

لاتنسونا من دعائكم

جميع حقوق النشر محفوظة لدى مؤسسة آفاق الإلكترونية 2018 ©
ولانبيح نسخ المواد العلمية والأمنية التى تقدمها المؤسسة دون ذكر المصدر